

Cyber Safety During Decommissioning at Indian Point Energy Center

**Dave Lochbaum
August 2022**

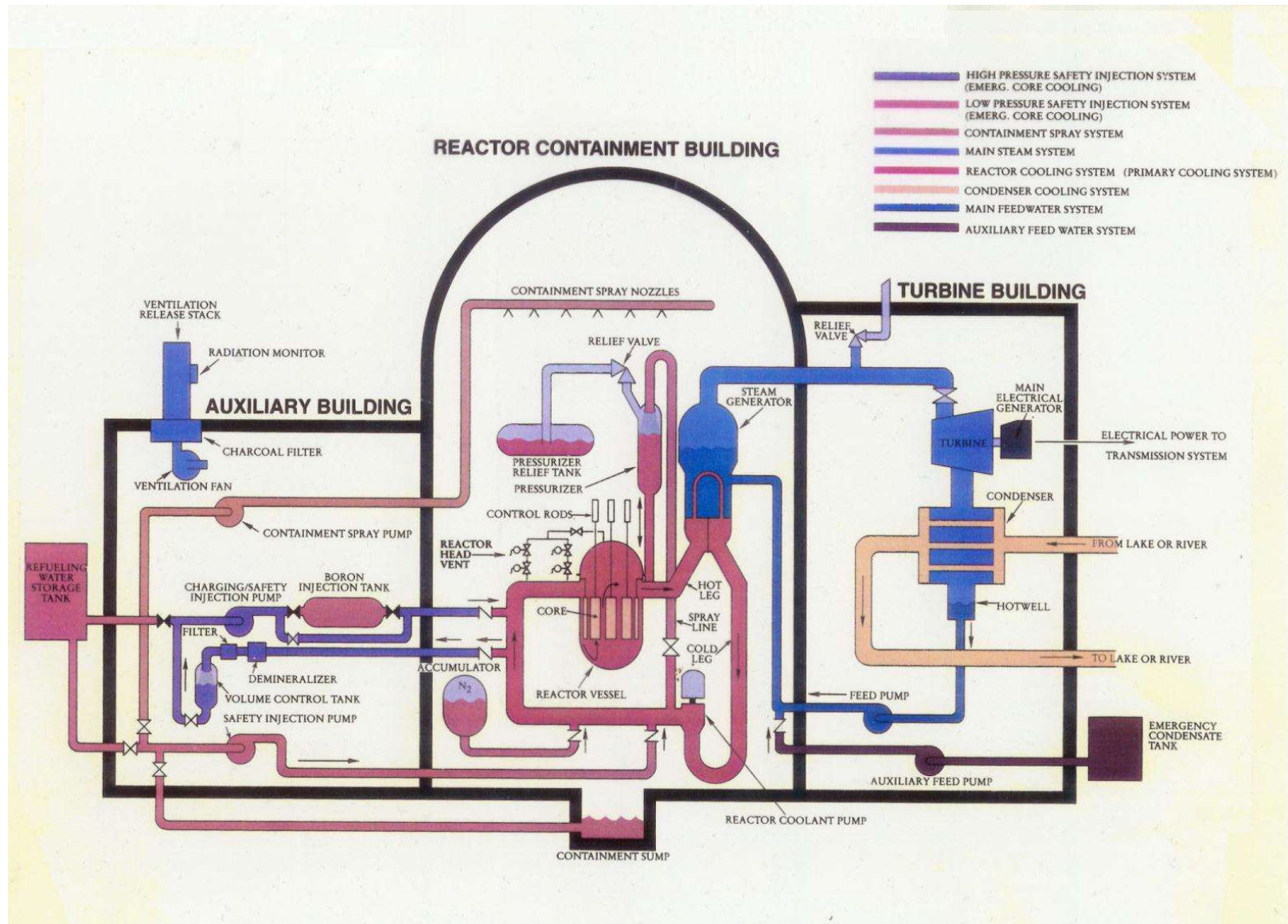
Cyber Security Rule

Following the 9/11 tragedy, then Nuclear Regulatory Commission (NRC) Chairman Richard Meserve announced the agency was conducting a top-to-bottom review of nuclear plant security regulations. The NRC issued Orders to nuclear plant owners requiring immediate security upgrades and initiated rulemaking to address additional measures, including cyber security.

On March 27, 2009, the NRC added §73.54 to Title 10 of the Code of Federal Regulations. This regulation, often called the Cyber Security Rule, required owners of nuclear power plants to submit a plan to the NRC by November 23, 2009, describing the steps to be taken to protect digital computer and communications systems that:

- 1. Perform safety-related and important-to-safety functions**
- 2. Perform security functions**
- 3. Perform emergency preparedness functions, including offsite communications**
- 4. Support systems and equipment which, if compromised, would adversely impact safety, security, and/or emergency preparedness functions**

Safety-Related and Important-to-Safety Functions



In this simplified drawing, safety-related and important-to-safety systems are shown in the Auxiliary and Reactor Containment Buildings while non-safety-related systems (with the exception of the Auxiliary Feed Pumps) are shown in the Turbine Building.

Security Functions



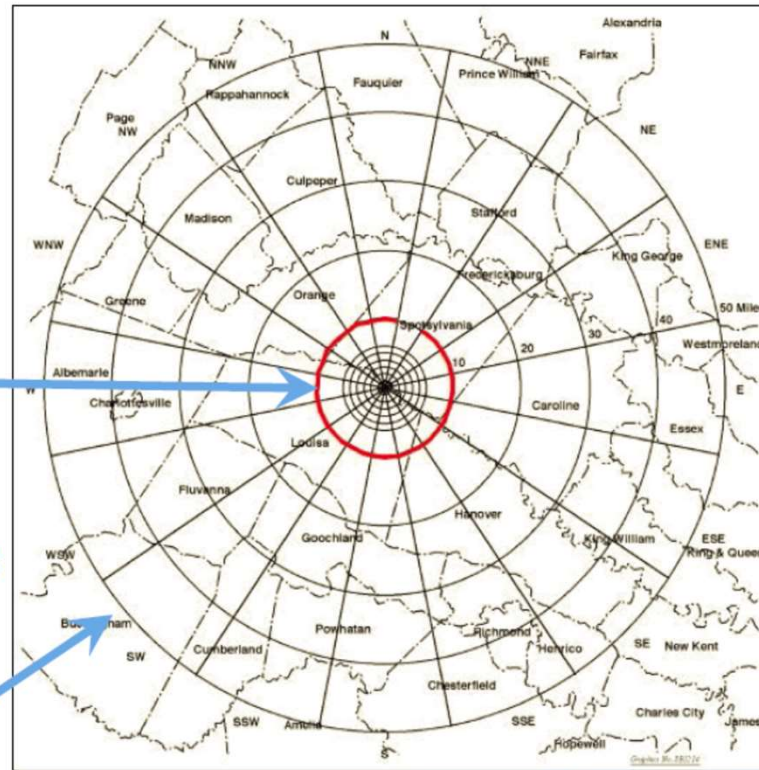
NRC's mandated security measures include gates, guard, and guns, but also include computer systems that limit access to vital rooms within the nuclear plant to only authorized persons.

Emergency Preparedness and Offsite Communications

Emergency Planning Zones (EPZs)



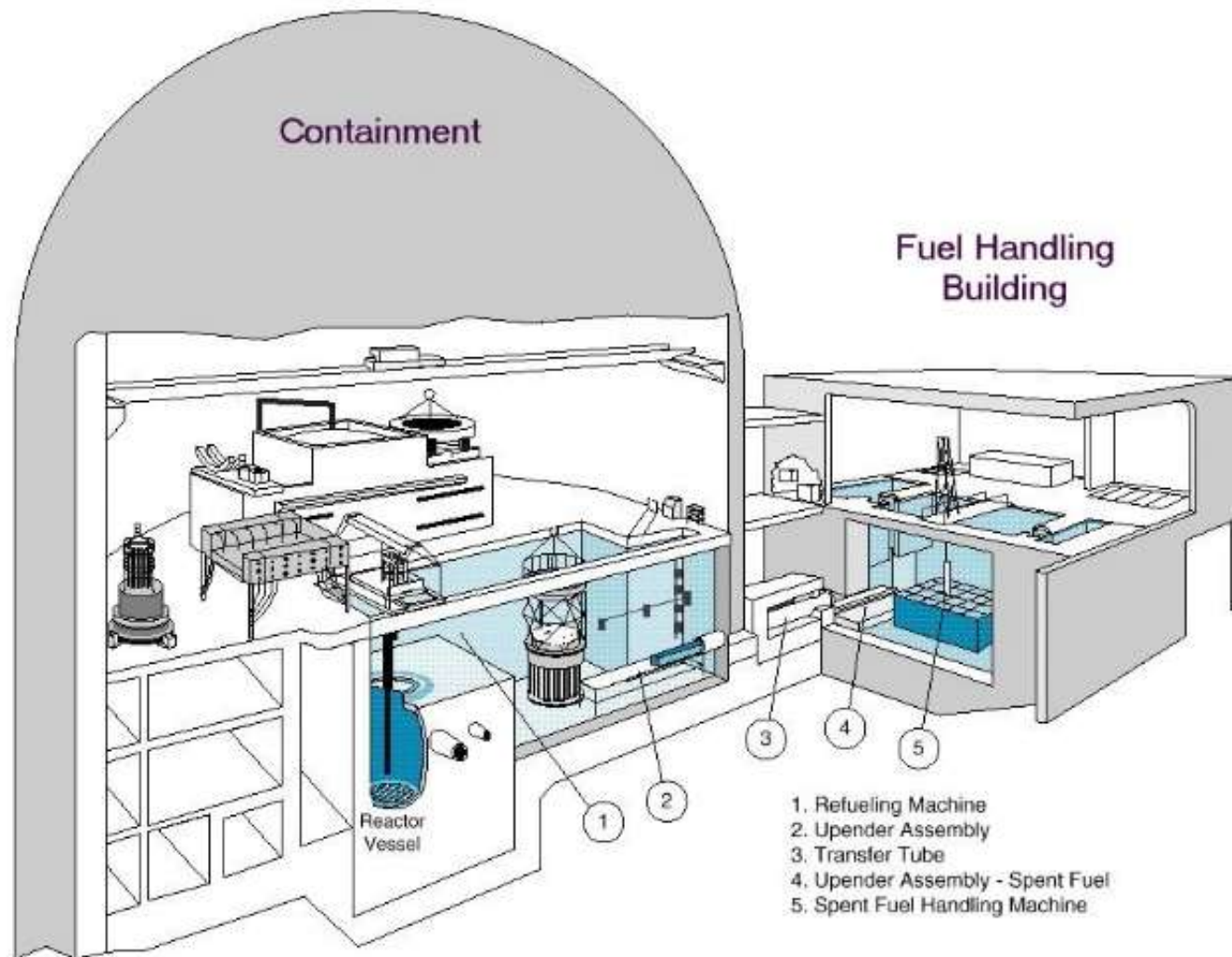
- Plume Exposure Pathway
 - 10 mile radius
- Ingestion Exposure Pathway
 - 50 mile radius



North Anna

Emergency preparedness requires actions by the nuclear plant owner (overseen by the NRC) and local, state, and federal responders (overseen by FEMA) to protect the public in event of a nuclear accident.

Support Systems and Equipment




As an example of a non-safety-related system whose failure could have adverse consequences, the spent fuel pool cooling system is classified non-safety-related. The spent fuel pool have sufficient cool water in it to protect the spent fuel from overheating damage.

Support Systems and Equipment



Another example of a non-safety-related system whose failure could have adverse consequences is the plant monitoring computer system. While dials, chart recorders, gauges, and indicators provide the same information, the monitoring computers provide it in a far more user-friendly and timely manner.

Cyber Security Threat



INL
Idaho National
Laboratory

INL/EXT-05-00671

Cyber Incidents Involving Control Systems

Robert J. Turk

October 2005

The INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance

Table 1. Control system-related terms in the MIPT database.

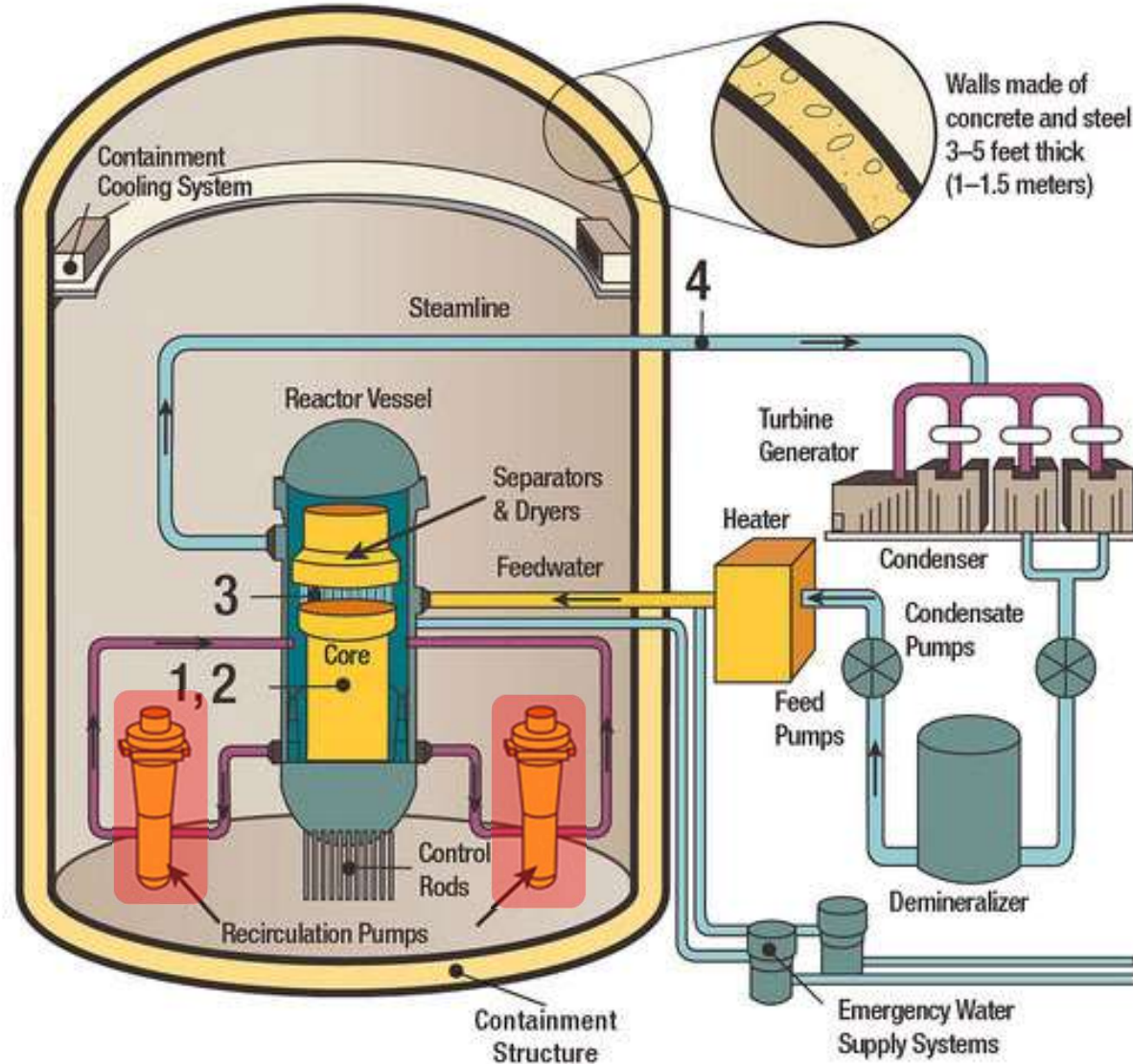
Search Term	Number of Hits
Process	62
Control	248
Process control	3
Remote	129
Remote control	95
Computer	23
PCS	0
SCADA	0
Cyber	0

Table 2. Events in the Energy Incident Database by type.

Category	No. of Events
Sabotage/terrorism	185
Disgruntled or striking employees	119
Vandalism/nuisance	57
Test and maintenance error	22
Fraud	12
Manager/operator decision	4
Equipment failure	3
Military take-over	6
Unknown	1
Total	409

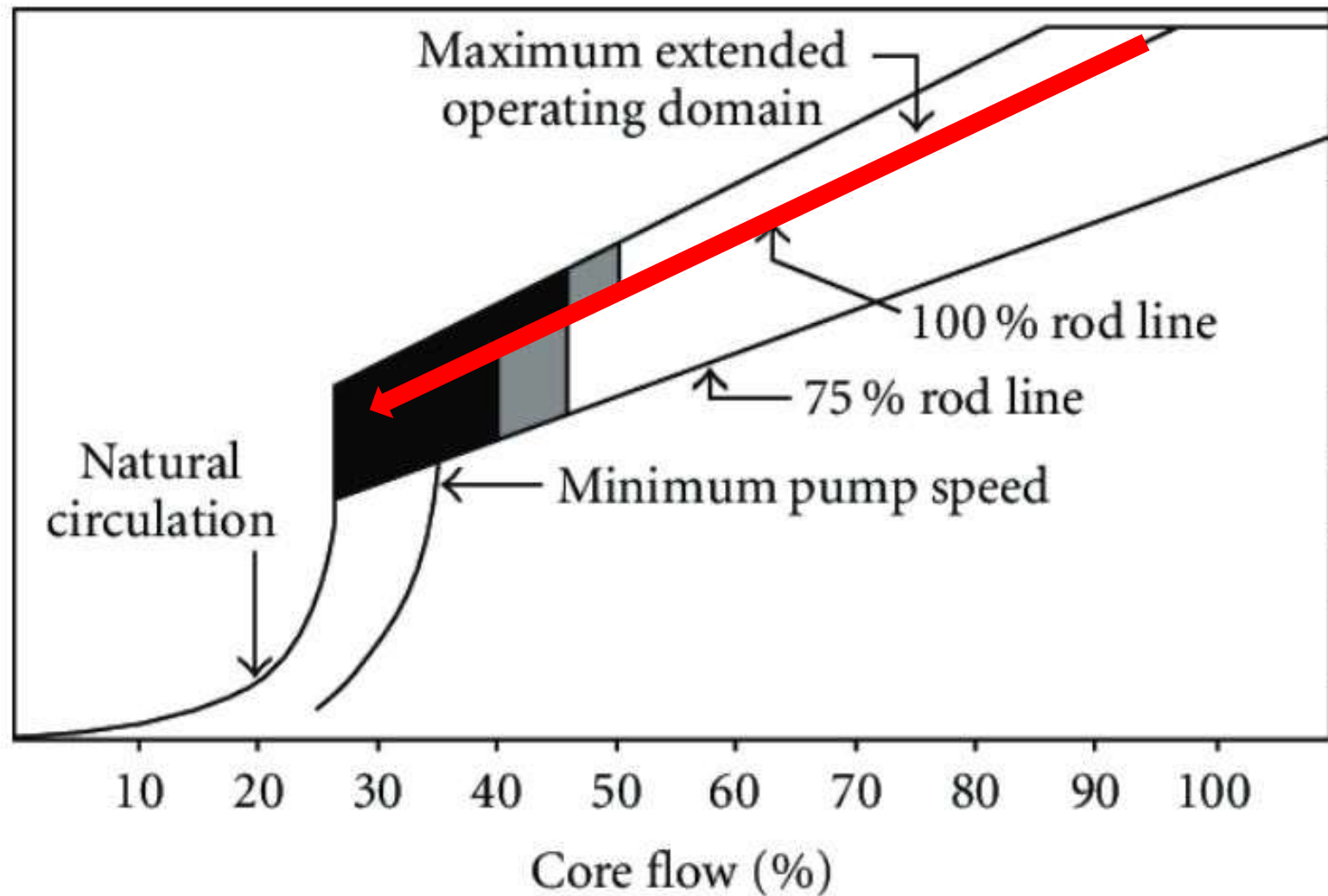
Although the 9/11 terrorists did not employ cyber security attacks, others had or were doing so, justifying the NRC's Cyber Security Rule.

Cyber Vulnerability



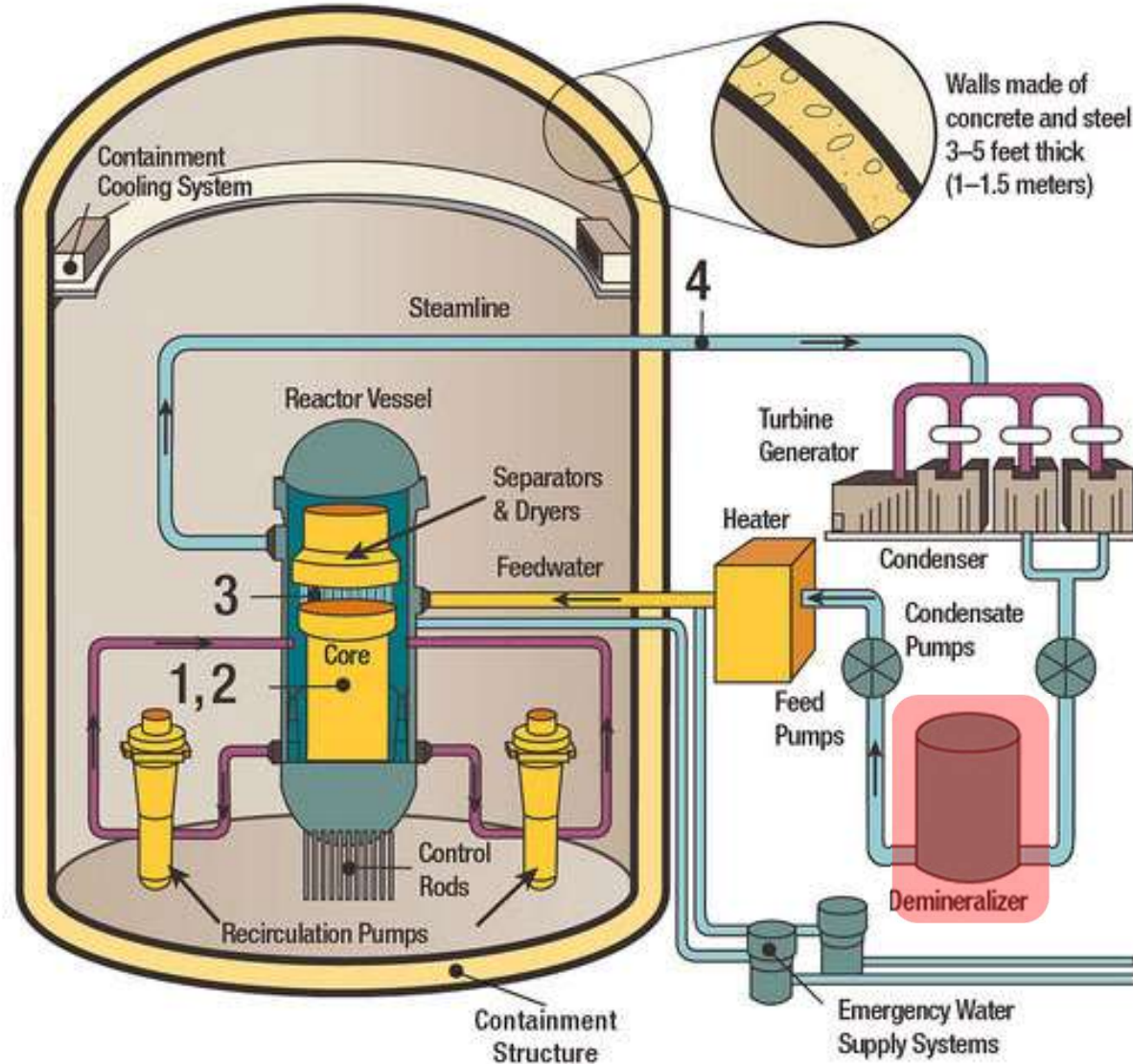
On August 19, 2006, the operators manually scrammed Browns Ferry Unit 3 following the loss of both of the recirculation pumps. These pumps circulate water through the reactor vessel and core to control power level.

Cyber Vulnerability



The loss of both recirculation pumps caused the reactor power level to decrease along the 100 percent rod line into a region of potential instability. Per procedure, the operators manually scrammed the reactor.

Cyber Vulnerability



The ensuing inquiry found that controls for the condensate demineralizers (one shown here to represent eight demins in service at full power) also locked up.

Cyber Vulnerability

The controls for the non-safety-related recirculation pumps and non-safety-related condensate demineralizers were connected to the site's computer network. Heavy traffic on this network caused the controls to "freeze up."

While this event was an accident cyber incident, it demonstrated that the computer network can be vulnerable to deliberate acts of malice.

The potential hazard of the cyber vulnerability at Browns Ferry was limited. Had the recirculation pumps increased flow through the core to increase the reactor power level, systems not connected to the site's computer network and not vulnerable to cyber shenanigans would have automatically scrambled the reactor before the higher power level caused fuel damage.

Similarly, had the demineralizer controls been manipulated for sinister purpose, systems not connected to the site's computer network would have automatically interceded before the consequences included reactor core damage.

The NRC alerted plant owners about this Browns Ferry incident and reminded owners *"it is important to protect both safety-related and non-safety related devices on the plant network to ensure the safe operation of the plant."*

Indian Point Compliance with Cyber Security Rule



Entergy Nuclear Northeast
Indian Point Energy Center
450 Broadway, GSB
P.O. Box 249
Buchanan, NY 10511-0249
Tel 914 734 6700

Joseph Pollock
Site Vice President
Administration

~~SECURITY-RELATED INFORMATION WITHHOLD UNDER 10 CFR 2.390~~

November 19, 2009

NL-09-147

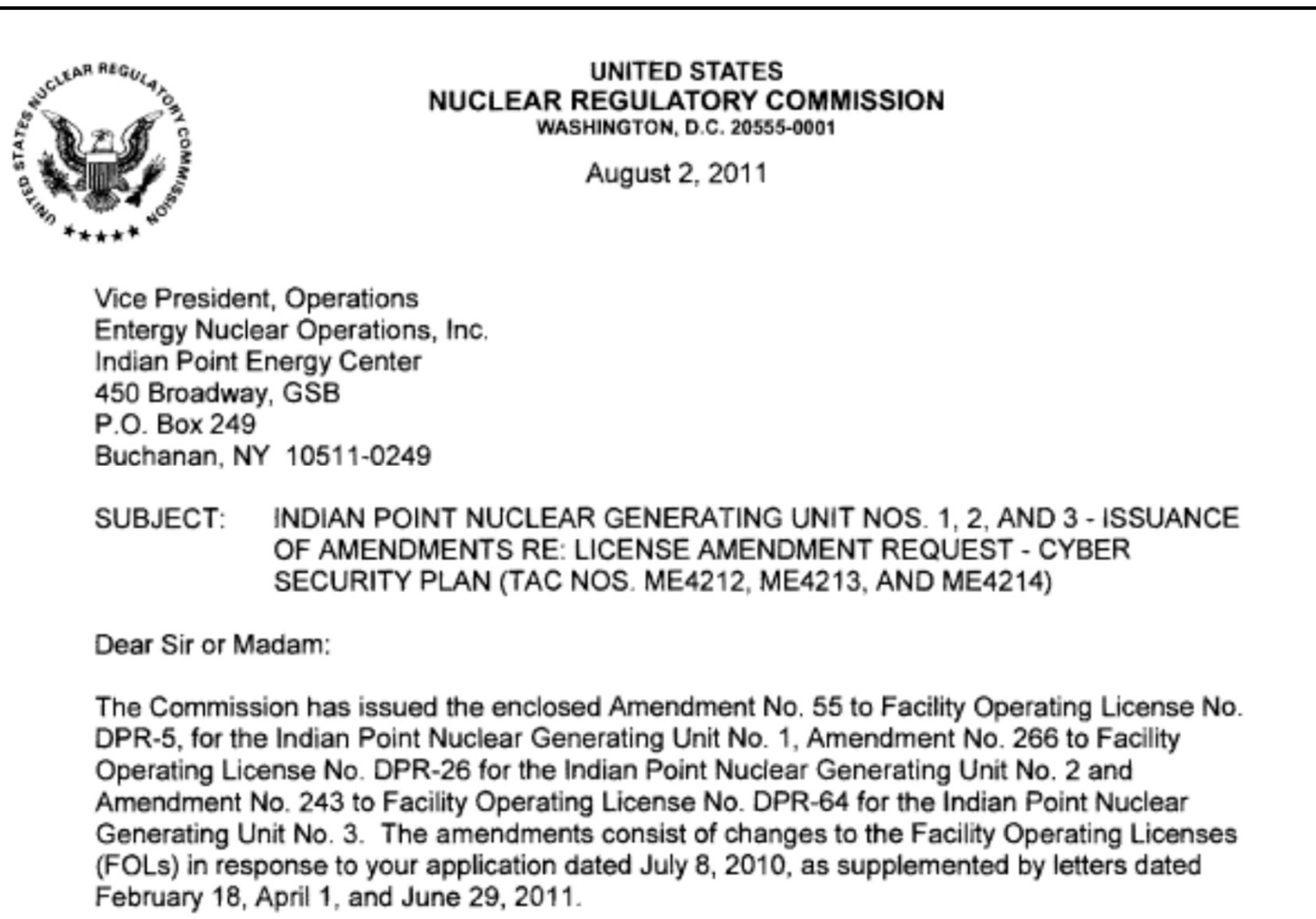
U.S. Nuclear Regulatory Commission
ATTN: Document Control Desk
Washington, DC 20555-0001

SUBJECT: Proposed License Amendment Regarding Cyber Security Plan
Indian Point Generating Unit Nos. 1, 2 and 3
Docket Nos. 50-003, 50-247 and 50-286
License Nos. DPR-5, DPR-26 and DPR-64

Dear Sir or Madam:

Ahead of the November 23, 2009 deadline, Entergy submitted its cyber security plan and associated implementation schedule to the NRC. The security-related information contained in the submittal was withheld from the public (and from bad guys).

Indian Point Compliance with Cyber Security Rule



On August 2, 2011, the NRC issued amendments approving the cyber security plan for Indian Point. The NRC evaluated the process used to identify computer and communications systems requiring protection, ongoing monitoring and assessment for these systems, how modifications to these systems will be controlled to sustain adequate protection, cyber security training programs, and other aspects en route to their approval.

NRC's Oversight of the Cyber Security Rule


Because information about cyber security in documents submitted to and issued by NRC is withheld from public disclosure, it's hard for the public to independently assess the effectiveness of the Cyber Security Rule and its implementation. The NRC's Inspector General can, and did, peek behind the curtain and audit NRC's oversight of cyber security:

The purpose of cyber security is to detect and then eliminate or mitigate vulnerabilities in digital systems that could be exploited either from outside or inside of a plant's protected area. Licensees operating a nuclear power plant are required to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber-attacks in accordance with 10 Code of Federal Regulations 73.54, which is also known as the "Cyber Security Rule."

The Office of the Inspector General (OIG) conducted this audit to determine the adequacy of the Nuclear Regulatory Commission's (NRC) cyber security inspection program for nuclear power plants. Through interviews with NRC staff, analysis, and direct observation, OIG auditors determined that NRC has adequate management controls in place for the cyber security inspection program. Therefore, OIG makes no recommendations.

It is rare, although not unprecedented, for the NRC Inspector not to find some problem to be rectified or some aspect to be enhanced. Comfort can be taken in the Inspector General determining NRC's oversight of cyber security to be adequate.

Indian Point Seeking Out of the Cyber Security Rule

	Krishna P. Singh Technology Campus, 1 Holtec Blvd., Camden, NJ 08104 Telephone (856) 797-0900 Fax (856) 797-0909
HDI-IPEC-22-039	10 CFR 50.90
May 20, 2022	
ATTN: Document Control Desk U.S. Nuclear Regulatory Commission Washington, DC 20555-0001	
Subject:	License Amendment Request – Revise License Condition to Eliminate Cyber Security Plan Requirements Indian Point Energy Center Provisional License No. DPR-5 Renewed Facility License No. DPR-26 and DPR-64 Docket Nos. 50-003, 50-247, and 50-286

On May 20, 2022, HOLTEC asked the NRC for permission to eliminate the cyber security plan for Indian Point and its requirements.

Indian Point Seeking Out of the Cyber Security Rule

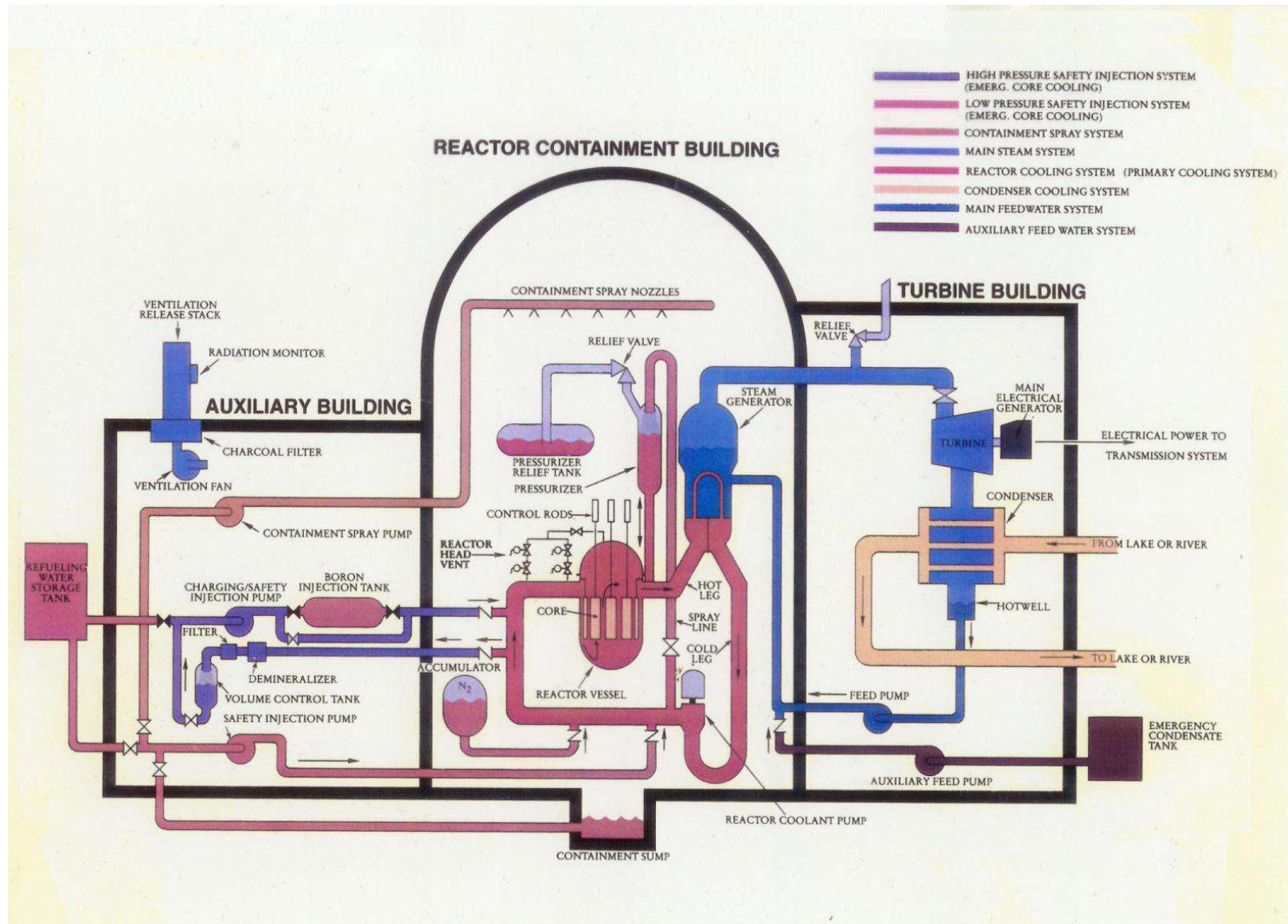
HOLTEC provided this basis for no longer needing the cyber security plan (CSP):

The regulatory and technical evaluations included in this LAR are consistent with recent NRC guidance on cyber security requirements for decommissioning facilities In addition, the NRC staff has approved similar LARs to delete the CSP license condition requirements from several 10 CFR 50 Licenses. For example, the NRC issued License Amendment for Three Mile Island Unit 1 dated December 4, 2020

The bounding analyses for the IP2 and IP3 SFPs for beyond design basis events demonstrate that 15 months after shutdown of IP3 a minimum of 10 hours is available before the fuel cladding temperature of the hottest fuel assembly in either SFP reaches 900°C with a complete loss of SFP water inventory Following the shutdown of the last unit (IP3), which occurred April 30, 2021, 15 months after IP3 shutdown would be July 30, 2022.

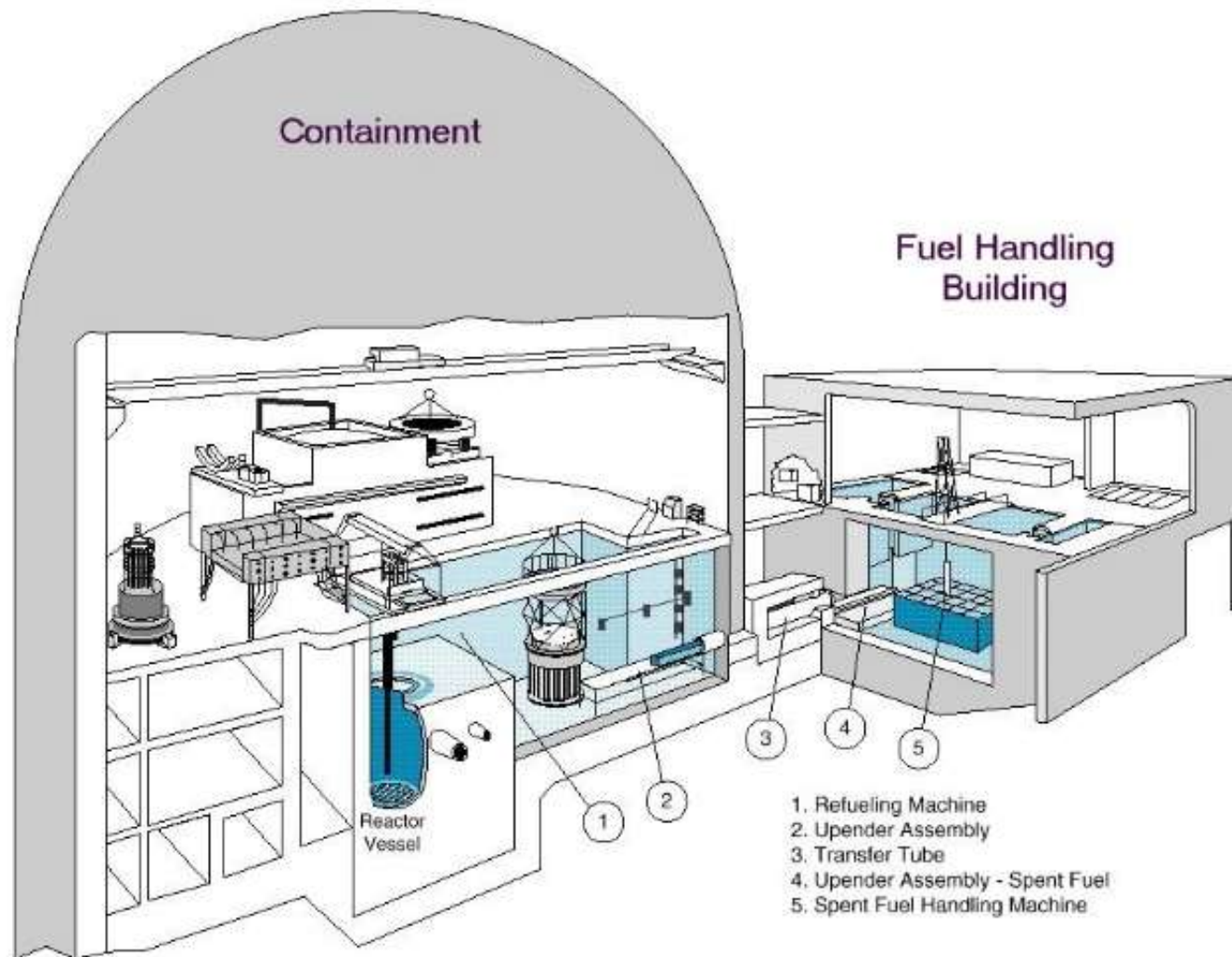
HDI requests approval of the proposed license amendment by January 31, 2023. The requested LAR approval date is prior to the anticipated completion of the transfer of all spent fuel from IP2 and IP3 to dry storage within the ISFSI, and after the appropriate cooling period for spent fuel in the SFP for both IP2 and IP3. Once approved, the license amendment will be implemented within 30 days of the date of the license amendment.

Safety-Related and Important-to-Safety Functions



With nuclear fuel permanently removed from the reactor vessels, the safety-related systems in the Auxiliary, Containment, and Turbine Buildings are no longer needed for its protection.

Support Systems and Equipment



Due to decay of radionuclides in the spent fuel pool since permanent shutdown of Units 2 and 3, there would be many hours available for workers to respond to loss of spent fuel pool cooling or spent fuel pool cooling water before overheating damage occurred.